Annales Mathematicae Silesianae 12 (1998), 105–121

Prace Naukowe Uniwersytetu Śląskiego nr 1751, Katowice

GENERATORS OF THE WITT GROUPS OF ALGEBRAIC INTEGERS

ALFRED CZOGAŁA

1. Introduction

For a number field K let $\mathcal{O}_K$ be the ring of algebraic integers of K. A basic result on the Witt ring $W\mathcal{O}_K$ of symmetric bilinear forms over the ring $\mathcal{O}_K$ was established in [MH]. The structure of the Witt group $W\mathcal{O}_K$, in terms of arithmetical invariants of K, was determined in [Sh]. Here we state precisely this description. We find generators of cyclic direct summands in the decomposition of the group $W\mathcal{O}_K$ into direct sum of cyclic groups. We will also describe products of these generators. This completely determines the structure of the ring $W\mathcal{O}_K$. As an illustration of these results we determine the structure of Witt rings $W\mathcal{O}_K$ for all quadratic, and some cubic and some biquadratic fields K. The results of this paper allow us to find arithmetical conditions for the existence of an isomorphism of Witt rings $W\mathcal{O}_K \to W\mathcal{O}_L$ (for details see [Cz2]).

2. Basic results on Witt rings of algebraic integers

If K is an algebraic number field, then the extension of scalars yields the Witt ring homomorphism $W\mathcal{O}_K \to WK$ which is injective and we have the Milnor-Knebusch exact sequence (see [MH, p. 93, 3.3, 3.4]):

$$0 \longrightarrow W\mathcal{O}_K \longrightarrow WK \xrightarrow{\partial} \sum_{\mathfrak{p}} W\overline{K}_{\mathfrak{p}} \longrightarrow C(K)/C(K)^2 \longrightarrow 1.$$

Received on September 15, 1998.

1991 *Mathematics Subject Classification.* 11E12.

Key words and phrases: Witt ring, ring of algebraic integers.

Supported by the State Committee for Scientific Research (KBN) of Poland under Grant 2 P03A 024 12.

Here the sum runs over all finite primes of K, whereas $\overline{K}_{\mathfrak{p}}$ and $C(K)$ denote the residue class field of the completion $K_{\mathfrak{p}}$ of K at $\mathfrak{p}$ and the ideal class group of K, respectively. The additive group homomorphism $\partial = \partial_K$ is the direct sum of the second residue class homomorphisms of Witt groups $\partial_{\mathfrak{p}} : WK \longrightarrow W\overline{K}_{\mathfrak{p}}$. Although the homomorphism $\partial_{\mathfrak{p}}$ depends on the choice of the local uniformizer at $\mathfrak{p}$, the kernel $\ker \partial_{\mathfrak{p}}$ does not depend on that choice. Hence the kernel of the homomorphism ∂_K does not depend on the choices of local uniformizers.

For this reason we can view the ring $W\mathcal{O}_K$ as a subring of the Witt ring of K and we will identify it with the kernel of ∂_K. This gives us the possibility to use classical methods and tools of the theory of quadratic forms over global fields (the Hasse-Witt invariant, the signature, the Local-Global Principle, Hilbert Reciprocity Law, etc.). In this way every element of the ring $W\mathcal{O}_K$ can be represented by a diagonal quadratic form $\langle a_1, \dots, a_n\rangle$ for some $n \in \mathbb{N}$ and $a_1, \dots, a_n \in K$. To simplify notation, we shall use the same symbol for the nonsingular symmetric bilinear form over K and its similarity class in the Witt ring WK. We denote by IK the fundamental ideal of WK consisting of even dimensional forms over K, by I^nK the nth power of IK and we set $I\mathcal{O}_K = IK \cap W\mathcal{O}_K$.

For a number field K, we write $r = r(K)$, $c = c(K)$, $g = g(K)$ for the number of infinite real primes, the number of pairs of infinite complex primes and the number of dyadic primes of K, respectively.

Let $\mathfrak{N}(WK)$ denote the nilradical of the ring WK. Then the set $\mathfrak{N}(W\mathcal{O}_K) = \mathfrak{N}(WK) \cap W\mathcal{O}_K$ is the nilradical of the ring $W\mathcal{O}_K$. The group $\mathfrak{N}(W\mathcal{O}_K)$ is a finite abelian group of order $2^{c+t+g-1}$, where $t = t(K)$ denotes the 2-rank of the ideal class group of K in the narrow sense (see [MH, Ch.4, §4]).

If K is totally imaginary (i.e. $r = 0$), then $\mathfrak{N}(W\mathcal{O}_K) = I\mathcal{O}_K$ and the dimension–index homomorphism produces the following exact sequence

$$(1) \qquad 0 \longrightarrow I\mathcal{O}_K \longrightarrow W\mathcal{O}_K \longrightarrow \mathbb{Z}/2\mathbb{Z} \to 0.$$

Therefore the group $W\mathcal{O}_K$ is a finite abelian group of order 2^{c+t+g}.

Now assume that the number field K is formally real (i.e. $r > 0$) and let $\sigma : WK \to \mathbb{Z}^r$ be total signature homomorphism. Then

$$\mathfrak{N}(W\mathcal{O}_K) = W\mathcal{O}_K \cap \ker \sigma$$

and $\sigma(W\mathcal{O}_K)$ is a free abelian group of rank r (cf. [MH, Ch.4, §4]). Then we have an exact sequence

$$(2) \qquad 0 \longrightarrow \mathfrak{N}(W\mathcal{O}_K) \longrightarrow W\mathcal{O}_K \longrightarrow \mathbb{Z}^r \longrightarrow 0$$

which splits. Hence the group $W\mathcal{O}_K$ is the direct sum of the group $\mathfrak{N}(W\mathcal{O}_K))$ and of some free abelian group A of rank r.

In the investigation of the Witt ring $W\mathcal{O}_K$ the group $K_{\mathrm{ev}}/\dot{K}^2$ plays a key role, where

$$K_{\mathrm{ev}} = \{x \in \dot{K} : \mathit{ord}_{\mathfrak{p}} x \equiv 0 \pmod 2 \text{ for every finite prime } \mathfrak{p} \text{ of } K\}.$$

The group $K_{\mathrm{ev}}/\dot{K}^2$ can be characterized as the set of values of the discriminant of forms belonging to $W\mathcal{O}_K$. This is the consequence of the following simple facts from [Sh, Proposition 2.4]:

If φ is form over K and $a \in \dot{K}$, then:

(1) $\varphi \in W\mathcal{O}_K \implies \mathit{disc}\varphi \in K_{\mathrm{ev}}/\dot{K}^2$,

(2) $\langle a\rangle \in W\mathcal{O}_K \iff a \in K_{\mathrm{ev}}$.

In [Cz2] we will show that the group $K_{\mathrm{ev}}/\dot{K}^2$ describes completely the isomorphism type of the ring $W\mathcal{O}_K$.

The group $K_{\mathrm{ev}}/\dot{K}^2$ is an elementary abelian 2-group and can be equipped with the structure of a linear space over the 2-element field $\mathbb{F}_2$. We will use frequently the same symbol for $x \in K_{\mathrm{ev}}$ and for its canonical image in $K_{\mathrm{ev}}/\dot{K}^2$. The 2-rank (the dimension over $\mathbb{F}_2$) of the group $K_{\mathrm{ev}}/\dot{K}^2$ is equal to $r + c + t'$, where $t' = t'(K)$ denotes the 2-rank of ideal class group of K (cf. [Cz1]). To construct a set of generators of the group $W\mathcal{O}_K$ we will use a suitably chosen basis of the group $K_{\mathrm{ev}}/\dot{K}^2$.

3. Generators of the group $\mathfrak{N}(W\mathcal{O}_K)$

In this section we find a decomposition of the group $\mathfrak{N}(W\mathcal{O}_K)$ into direct sum of cyclic groups and we describe generators of cyclic summands. Observe that $4 \cdot \mathfrak{N}(W\mathcal{O}_K) \subset I^3K \cap \mathfrak{N}(WK) = 0$, hence the order of every element of $\mathfrak{N}(W\mathcal{O}_K)$ divides 4.

Let K_+ denote the set of totally positive elements of K. From [MH, Lemma 4.6] it follows that the discriminant $\mathit{disc} : IK \to \dot{K}/\dot{K}^2$ induces a group isomorphism

$$\mathfrak{N}(W\mathcal{O}_K)/\,\mathfrak{N}(W\mathcal{O}_K) \cap I^2K \longrightarrow K_{\mathrm{ev}} \cap K_+/\dot{K}^2 \tag{3}$$

whose inverse sends the square class of a onto the coset of the binary form $\langle 1, -a\rangle$. The 2-rank of the group $K_{\mathrm{ev}} \cap K_+/\dot{K}^2$ is equal to $c + t$ (cf. [MH, Ch.4, §4]). If we choose a basis $\{a_1, \dots, a_{c+t}\}$ for this group, then the cosets of the forms $\langle 1, -a_1\rangle, \dots, \langle 1, -a_{c+t}\rangle$ will be generators of cyclic summands in the decomposition of the quotient group $\mathfrak{N}(W\mathcal{O}_K)/\,\mathfrak{N}(W\mathcal{O}_K) \cap I^2K$ into direct sum of cyclic groups.

For a prime $\mathfrak{p}$ of K, let $h_{\mathfrak{p}} : I^2K \to \{\pm 1\}$ be the $\mathfrak{p}$-adic Hasse-Witt invariant homomorphism. Assume that $\mathfrak{p}_1, \dots, \mathfrak{p}_g$ are all dyadic primes of K and denote the group $\{\pm 1\}^{g-1}$ by Γ_K. The map

$$H : \mathfrak{N}(W\mathcal{O}_K) \cap I^2K \to \Gamma_K, \quad H(\varphi) = (h_{\mathfrak{p}_1}(\varphi), \dots, h_{\mathfrak{p}_{g-1}}(\varphi))$$

is a group isomorphism (see [MH, Lemma 4.5]), so the order of the group $\mathfrak{N}(W\mathcal{O}_K) \cap I^2K$ is equal to 2^{g-1}.

From [Sh, Proposition 2.6] it follows, that there exists an isomorphism

$$(4) \qquad K_{\mathrm{ev}} \cap K_+/K_{\mathrm{ev}} \cap D_K\langle 1,\,1\rangle \longrightarrow 2\cdot\mathfrak{N}(W\mathcal{O}_K), \quad \bar{a} \mapsto 2\cdot\langle 1,\,-a\rangle,$$

where $D_K\langle 1,\,1\rangle$ denotes the set of elements represented by the form $\langle 1,\,1\rangle$.

Therefore, if $a \in K_{\mathrm{ev}} \cap K_+$ is a nonsquare in K, then the binary form $\langle 1,\,-a\rangle \in \mathfrak{N}(W\mathcal{O}_K)$ is an element of order 2 when $a \in D_K\langle 1,\,1\rangle$, and of order 4 otherwise.

The Hasse Local-Global Principle and the properties of Hilbert symbols give a simple description of the group $K_{\mathrm{ev}} \cap D_K\langle 1,\,1\rangle$ by means of dyadic Hilbert symbols:

$$K_{\mathrm{ev}} \cap D_K\langle 1,\,1\rangle = \{a \in K_{\mathrm{ev}} \cap K_+ : (-1,\,a)_{\mathfrak{p}} = 1 \text{ for all dyadic primes } \mathfrak{p}\}.$$

The group $K_{\mathrm{ev}} \cap K_+/K_{\mathrm{ev}} \cap D_K\langle 1,\,1\rangle$ is an elementary abelian 2-group. The 2-rank of this group we will denoted $u = u(K)$. From the inclusion $2\cdot\mathfrak{N}(W\mathcal{O}_K) \subset \mathfrak{N}(W\mathcal{O}_K) \cap I^2K$ it follows that $u \leqslant g-1$.

For further consideration we choose a basis $\{a_1, \ldots, a_{c+t}\}$ of the group $K_{\mathrm{ev}} \cap K_+/\dot{K}^2$ so that the elements $a_{u+1}, \ldots, a_{c+t}$ belong to $K_{\mathrm{ev}} \cap D_K\langle 1,\,1\rangle$ (when $u < c+t$). Then the elements $a_1, \ldots, a_u$ form a basis of the group $K_{\mathrm{ev}} \cap K_+/K_{\mathrm{ev}} \cap D_K\langle 1,\,1\rangle$ (when $u > 0$).

We have the following decomposition of the group $2\cdot\mathfrak{N}(W\mathcal{O}_K)$ into direct sum of cyclic groups:

$$(5) \qquad 2\cdot\mathfrak{N}(W\mathcal{O}_K) = \bigoplus_{i=1}^{u}(2\langle 1,\,-a_i\rangle).$$

The symbol (φ) denotes the cyclic group generated by the element φ.

Lemma 3.1. *Let E denote the subgroup of $\mathfrak{N}(W\mathcal{O}_K)$ generated by the forms $\langle 1,\,-a_1\rangle, \ldots, \langle 1,\,-a_{c+t}\rangle$. Then*

$$E = \bigoplus_{i=1}^{c+t}(\langle 1,\,-a_i\rangle) \quad \textit{and} \quad E \cap I^2K = 2\cdot\mathfrak{N}(W\mathcal{O}_K).$$

Proof. Assume that for some integers $k_1, \ldots, k_{c+t}$ the form

$$\varphi = \sum_i k_i\langle 1,\,-a_i\rangle$$

belongs to I^2K. Then $disc\varphi = a_1^{k_1}\dots a_{c+t}^{k_{c+t}}$ is a square and so the numbers $k_1,\dots,k_{c+t}$ are all even. Therefore φ is an element of the group $2\cdot\mathfrak{N}(W\mathcal{O}_K)$.

To complete the proof assume $\sum_{i=1}^{c+t} k_i\langle 1, -a_i\rangle = 0$. From the above it follows that $k_i = 2k_i'$, $i = 1,\dots,c+t$. Since the forms $\langle 1, -a_{u+1}\rangle,\dots,\langle 1, -a_{c+t}\rangle$ are elements of order 2, we have $\sum_{i=1}^{u} k_i'\cdot 2\langle 1, -a_i\rangle = 0$. This equality and the isomorphism (4) imply that the numbers $k_1',\dots,k_u'$ are all even, so the numbers $k_1,\dots,k_u$ are all divisible by 4. □

Clearly, the forms $2\langle 1, -a_i\rangle$, $i = 1,\dots,u$ generate the direct summands of the group $\mathfrak{N}(W\mathcal{O}_K)\cap I^2K$. If $u < g-1$ we will show that some suitably chosen 2-fold Pfister forms form a set of generators of the remaining direct summands (we write $\langle\langle a, b\rangle\rangle = \langle 1, a\rangle\otimes\langle 1, b\rangle$).

Denote $\alpha_i = H(2\langle 1, -a_i\rangle) = H(\langle\langle 1, -a_i\rangle\rangle)\in\Gamma_K$, $i = 1,\dots,u$, (when $u > 0$). Notice that the set $\{\alpha_1,\dots,\alpha_u\}$ is linearly independent over $\mathbb{F}_2$. Indeed, linear dependence would imply the equality $(-1, a_{i_1}\dots a_{i_k})_{\mathfrak{p}} = 1$ for some $i_1,\dots,i_k\in\{1,\dots,u\}$ and every dyadic prime $\mathfrak{p}$. This implies that $a_{i_1}\dots a_{i_k}\in D_K\langle 1, 1\rangle$ and contradicts the choice of the elements $a_1,\dots,a_u$.

When $u < g-1$ we complete the set $\{\alpha_1,\dots,\alpha_u\}$ to a basis

$$\{\alpha_1,\dots,\alpha_{g-1}\}$$

of the group Γ_K. The Approximation Theorem guarantees the existence of an element $f\in K$ such that $-f$ is totally positive and $-f$ is nonsquare in every dyadic completion of field K. From [OM, 71:19] it follows that there exist elements $d_{u+1},\dots,d_{g-1}\in K$ such that $H(\langle\langle f, d_i\rangle\rangle) = \alpha_i$ for $i = u+1,\dots,g-1$ and $h_{\mathfrak{q}}(\langle\langle f, d_i\rangle\rangle) = (-f, -d_i)_{\mathfrak{q}} = 1$ for every nondyadic finite prime $\mathfrak{q}$.

For a nondyadic finite prime $\mathfrak{q}$ the Hasse-Witt invariant $h_{\mathfrak{q}}$ can be identified with the second residue class homomorphism $\partial_{\mathfrak{q}}$ (cf. [MH, Ch.4, §4]). So we have $\partial_{\mathfrak{q}}(\langle\langle f, d_i\rangle\rangle) = 0$. Moreover, if $r > 0$, then the total signature homomorphism vanishes on the form $\langle\langle f, d_i\rangle\rangle$, because f is totally negative. Hence $\langle\langle f, d_i\rangle\rangle$ is an element of $\mathfrak{N}(W\mathcal{O}_K)\cap I^2K$ for every $i\in\{u+1,\dots,g-1\}$.

Using the above construction we obtain the following decomposition of the group $\mathfrak{N}(W\mathcal{O}_K)\cap I^2K$:

$$\mathfrak{N}(W\mathcal{O}_K)\cap I^2K = \bigoplus_{i=1}^{u}(2\langle 1, -a_i\rangle)\oplus\bigoplus_{i=u+1}^{g-1}\langle\langle f, d_i\rangle\rangle. \tag{6}$$

Corollary 3.1. *If the elements $a_1,\dots,a_{c+t}, f, d_{u+1},\dots,d_{g-1}$ are chosen as above, then*

$$\mathfrak{N}(W\mathcal{O}_K) = \bigoplus_{i=1}^{c+t}(\langle 1, -a_i\rangle)\oplus\bigoplus_{i=u+1}^{g-1}(\langle\langle f, d_i\rangle\rangle).$$

If $u = g-1$, then the last summand in the decomposition does not occur. In the above decomposition, the generators $\langle 1, -a_1\rangle, \dots, \langle 1, -a_u\rangle$ are elements of order 4, and the remaining generators have the order 2.

We will now describe the products of the generators of $\mathfrak{N}(WO_K)$ occurring in the above decomposition. To simplify the notation we write $\varphi_i = \langle 1, -a_i\rangle$, $i = 1, \dots, c+t$ and $\phi_i = \langle\langle f, d_i\rangle\rangle$, $i = u+1, \dots, g-1$. For every $i \in \{1, \dots, c+t\}$, $j, k \in \{u+1, \dots, g-1\}$, the elements $\varphi_i\phi_j$, $\phi_j\phi_k$ belong to $\mathfrak{N}(WO_K) \cap I^3K = 0$, hence $\varphi_i\phi_j = 0$ and $\phi_j\phi_k = 0$. Clearly $\varphi_i\varphi_i = 2\varphi_i$ for $i = 1, \dots, c+t$.

It remains to describe the products $\varphi_i\varphi_j$ for $i, j \in \{1, \dots, c+t\}$, $i \neq j$. It is easily seen that the product $\varphi_i\varphi_j$ belongs to the group $\mathfrak{N}(WO_K) \cap I^2K$. So it is completely determined by the value of $H(\varphi_i\varphi_j) \in \Gamma_K$. Hence, if $H(\varphi_i\varphi_j) = \prod_{i=1}^{u} \alpha_i^{k_i} \cdot \prod_{j=u+1}^{g-1} \alpha_j^{l_j}$, where $k_i, l_j \in \{0, 1\}$, then we have $\varphi_i\varphi_j = \sum_{i=1}^{u} 2k_i\varphi_i + \sum_{j=u+1}^{g-1} l_j\phi_j$.

4. Generators of the group WO_K in the nonreal case

When K is a totally imaginary algebraic number field (i.e. $r = 0$), then $\mathfrak{N}(WO_K) = IO_K$. The structure of the group WO_K depends on the level $s = s(K)$ of K. Thus we will consider 3 cases. We use the notation of the previous sections.

Case: $s = 4$. The form $\langle 1\rangle$ is an element of order 8 and there are at least 2 dyadic primes in K $(g \geqslant 2)$. In this case -1 is not represented by the form $\langle 1, 1\rangle$, hence $u \geqslant 1$ and we take $a_1 = -1$. We have the group isomorphism $WO_K \cong (\langle 1\rangle) \oplus WO_K/(\langle 1\rangle)$. Since $IO_K \cap (\langle 1\rangle) = (\langle 1, 1\rangle)$, there exists the group monomorphism $IO_K/(\langle 1, 1\rangle) \to WO_K/(\langle 1\rangle)$. This monomorphism is actually an isomorphism, because the orders of both groups coincide (are equal to $2^{c+t+g-3}$). Therefore we obtain the following decomposition:

$$WO_K = (\langle 1\rangle) \oplus \bigoplus_{i=2}^{c+t} (\langle 1, -a_i\rangle) \oplus \bigoplus_{i=u+1}^{g-1} (\langle\langle f, d_i\rangle\rangle). \tag{7}$$

Case: $s = 2$. In this case the form $\langle 1\rangle$ is an element of order 4 and $-1 \in D_K\langle 1, 1\rangle$. Hence $u < c+t$ and we take $a_{c+t} = -1$. Similarly as in the previous case we get the following decomposition:

$$WO_K = (\langle 1\rangle) \oplus \bigoplus_{i=1}^{c+t-1} (\langle 1, -a_i\rangle) \oplus \bigoplus_{i=u+1}^{g-1} (\langle\langle f, d_i\rangle\rangle). \tag{8}$$

Case: $s = 1$. In this case $K_{ev} \subset D_K\langle 1, 1\rangle$, so $u = 0$. Thus the group WO_K is an elementary abelian 2-group and in this case we have

$$WO_K = (\langle 1\rangle) \oplus \bigoplus_{i=1}^{c+t} (\langle 1, -a_i\rangle) \oplus \bigoplus_{i=1}^{g-1} (\langle\langle f, d_i\rangle\rangle). \tag{9}$$

5. Generators of the group WO_K in the real case

In this section we assume that the algebraic number field K is formally real (i.e. $r(K) > 0$). Recall that $WO_K = A \oplus \mathfrak{N}(WO_K)$, where A is a free abelian group of rank r. We will find a basis for the group A.

Let $\infty_1, \dots, \infty_r$ be the all infinite real primes of K and for $a \in \dot{K}$, let $sign_{\infty_i}(a)$ denote the sign of the element a in the ordering determined by the real prime ∞_i. The order of the group $K_{ev}/K_{ev} \cap K_+$ is equal to $2^{r-(t-t')}$ (cf. [Cz1]). Let $\rho = r - (t - t')$. There exist infinite real primes $\infty_1, \dots, \infty_\rho$ and elements $b_2, \dots, b_\rho \in K_{ev}$ such that b_i is negative at ∞_i and positive at ∞_j for all $i \in \{2, \dots, \rho\}$, $j \in \{1, \dots, \rho\}$, $i \neq j$.

From [Sh, Proposition 3.4] it follows that $\sigma(WO_K) = \sigma(WK))$ iff $r = \rho$. It is easy to verify that in this case the one dimensional forms $\langle 1\rangle, \langle b_2\rangle, \dots, \langle b_r\rangle$, form a basis of the group A. Thus we have

COROLLARY 5.1. *If the rank of the group $K_{ev}/K_{ev} \cap K_+$ is equal to r and $b_2, \dots, b_r \in K_{ev}$ are chosen as above, then*

$$WO_K = (\langle 1\rangle) \oplus \bigoplus_{i=2}^{r} (\langle b_i\rangle) \oplus \mathfrak{N}(WO_K).$$

Now we will assume that $\rho < r$. Clearly the forms $\langle 1\rangle, \langle b_2\rangle, \dots, \langle b_\rho\rangle$ are linearly independent (over $\mathbb{Z}$) elements of the group A. We will show that this set of form can be completed to a basis of the group A by a set of binary forms.

LEMMA 5.1. *Assume that we have $\epsilon_1, \dots, \epsilon_r \in \{\pm 1\}$ and $v_\mathfrak{p} \in \dot{K}_\mathfrak{p}$ for every dyadic prime $\mathfrak{p}$ of K. Then there exists an element $q \in K$ and a nondyadic prime $\mathfrak{q}$ of K such that*

(1) $sign_{\infty_i}(q) = \epsilon_i$ *for* $i = 1, \dots, r$,

(2) $q = v_\mathfrak{p} \bmod \dot{K}^2\mathfrak{p}$ *for every dyadic prime* $\mathfrak{p}$,

(3) $\mathrm{ord}_\mathfrak{q} q = 1$,

(4) $\mathrm{ord}_\mathfrak{r} q = 0$ *for every nondyadic prime* $\mathfrak{r} \neq \mathfrak{q}$.

PROOF. The Approximation Theorem [L, p. 35] yields an element α in $\dot{K}$ such that $sign_{\infty_i}(\alpha) = \epsilon_i$ for $i = 1, \dots, r$ and $\alpha \dot{K}_\mathfrak{p}^2 = v_\mathfrak{p} \dot{K}_\mathfrak{p}^2$ for every dyadic prime $\mathfrak{p}$. Suppose the principal ideal generated by α has the decomposition

$$\alpha O_K = \mathfrak{J} \cdot \prod_{\mathfrak{p}|2} \mathfrak{p}^{l_\mathfrak{p}}$$

where $\mathfrak{I}$ is a fractional ideal coprime with all dyadic primes of K, and $l_\mathfrak{p} \in \mathbb{Z}$. Consider the cycle $\mathfrak{c} = \prod_\mathfrak{p} \mathfrak{p}^{m_\mathfrak{p}}$ such that

$$m_\mathfrak{p} = \begin{cases} 1 & \text{if } \mathfrak{p} \text{ is an infinite real prime} \\ 2e_\mathfrak{p}(K)+1 & \text{if } \mathfrak{p} \text{ is a dyadic prime} \\ 0 & \text{otherwise} \end{cases}$$

where $e_\mathfrak{p}(K)$ denotes the ramification index of $\mathfrak{p}$ in K.

The class of the ideal $\mathfrak{I}$ in the generalized ideal class group $I(\mathfrak{c})/K_\mathfrak{c}$ contains infinitely many prime ideals (c.f. [L, p. 166-167]). Let $\mathfrak{q}$ be a nondyadic prime belonging to this class. According to the definition of the generalized ideal class group we have $\mathfrak{q} = \mathfrak{I} \cdot \gamma \mathcal{O}_K$ for certain $\gamma \in \dot{K}$ such that $\gamma \equiv 1 \pmod{{}^*\mathfrak{c}}$. Since $\gamma \in 1 + 4\mathfrak{p}$ for all dyadic primes $\mathfrak{p}$, the Hensel Lemma [L, p. 42] guarantees that $\gamma \in \dot{K}_\mathfrak{p}^2$. Taking $q = \alpha\gamma$, we have $q = \alpha \bmod \dot{K}_\mathfrak{p}^2$ for every dyadic prime $\mathfrak{p}$ and

$$q\mathcal{O}_K = \alpha\gamma\mathcal{O}_K = \mathfrak{I} \cdot \gamma\mathcal{O}_K \prod_{\mathfrak{p}|2} \mathfrak{p}^{l_\mathfrak{p}} = \mathfrak{q} \prod_{\mathfrak{p}|2} \mathfrak{p}^{l_\mathfrak{p}}.$$

This proves (2), (3) and (4). The element γ is totally positive, hence $sign_{\infty_i}(q) = sign_{\infty_i}(\alpha) = \epsilon_i$ and (1) is also fulfilled. □

LEMMA 5.2. *There exists an element $z \in K_{\mathrm{ev}} \cap K_+$ and a dyadic prime $\mathfrak{p}_0$ such that $-z$ is a nonsquare in $K_{\mathfrak{p}_0}$.*

PROOF. If -1 is a nonsquare in a dyadic completion of K, then we take $z = 1$.

Now assume that -1 is a square in every dyadic completion of K. Let K_{sq} denote the set of elements of $K_{\mathrm{ev}} \cap K_+$ which are squares in all dyadic completions of K, and let $\delta = \delta(K)$ denote the 2-rank of the subgroup of ideal class group generated by classes of all dyadic ideals of K. From [Cz1] it follows that 2-rank of the group $K_{\mathrm{ev}} \cap K_+/K_{sq}$ is equal to $c + (t - t') + \delta$, and it is nonzero, since $t - t' > 0$. Hence there exists a dyadic prime $\mathfrak{p}_0$ and a $z \in K_{\mathrm{ev}} \cap K_+$ such that z is a nonsquare in $K_{\mathfrak{p}_0}$. Then $-z$ is also a nonsquare in $K_{\mathfrak{p}_0}$.

For further consideration we fix an element $e \in K_{\mathrm{ev}}$, a dyadic prime $\mathfrak{p}_0$ of K and an element $v \in \dot{K}_{\mathfrak{p}_0}$ such that $-e \in K_{\mathrm{ev}} \cap K_+$, $e \notin \dot{K}_{\mathfrak{p}_0}^2$ and $(e, v)_{\mathfrak{p}_0} = -1$. □

From Lemma 5.1 it follows that for every $i \in \{\rho + 1, \dots, r\}$ there exists a nondyadic prime $\mathfrak{q}_i$ and an element $q_i \in \dot{K}$ such that:

(1) $sign_{\infty_i}(q_i) = -1$, $sign_{\infty_j}(q_i) = 1$, for $j = 1, \dots, r$, $j \neq i$;

(2) $q_i = v \bmod \dot{K}_{\mathfrak{p}_0}^2$;
(3) $q_i = 1 \bmod \dot{K}_{\mathfrak{p}}^2$, for every dyadic prime $\mathfrak{p} \neq \mathfrak{p}_0$;
(4) $ord_{\mathfrak{q}_i} q_i = 1$;
(5) $ord_{\mathfrak{r}} q_i = 0$, for every nondyadic prime $\mathfrak{r} \neq \mathfrak{q}_i$.

LEMMA 5.3. *If e, b_i and q_i are as above, then the forms*

$$\langle 1\rangle, \langle b_1\rangle, \ldots, \langle b_{\rho-1}\rangle, \langle q_{\rho+1}, -eq_{\rho+1}\rangle, \ldots, \langle q_r, -eq_r\rangle \tag{10}$$

form a basis for the free abelian group A.

PROOF. First we will show that $\langle q_i, -eq_i\rangle \in WO_K$, for $i = \rho+1, \ldots, r$. The properties (1) – (5) imply the following equalities of Hilbert symbols:
$(q_i, -eq_i)_{\infty_i} = -1$,
$(q_i, -eq_i)_{\mathfrak{p}_0} = (q_i, e)_{\mathfrak{p}_0} = -1$,
$(q_i, -eq_i)_{\mathfrak{r}} = 1$, for every prime $\mathfrak{r} \neq \infty_i, \mathfrak{p}_0, \mathfrak{q}_i$.
Thus the Hilbert Reciprocity implies $(q_i, e)_{\mathfrak{q}_i} = (q_i, -eq_i)_{\mathfrak{q}_i} = 1$. Therefore the element e is a local square at $\mathfrak{q}_i$ and we have $\partial_{\mathfrak{q}_i}(\langle q_i, -eq_i\rangle) = \langle \overline{q}_i, -\overline{q}_i\rangle = 0$. The elements q_i, $-eq_i$ are $\mathfrak{r}$-units modulo square for every nondyadic prime $\mathfrak{r} \neq \mathfrak{q}_i$, hence $\partial_{\mathfrak{r}}(\langle q_i, -eq_i\rangle) = 0$. For every dyadic prime $\mathfrak{p}$ the fundamental ideal $IK_{\mathfrak{p}}$ is equal to 0, so $\partial_{\mathfrak{p}}(\langle q_i, -eq_i\rangle) = 0$. Finally $\langle q_i, -eq_i\rangle \in \ker \partial_K$.

To simplify notation we will denote the forms $\langle 1\rangle$, $\langle b_2\rangle, \ldots, \langle b_{\rho-1}\rangle$, $\langle q_{\rho+1}, -eq_{\rho+1}\rangle, \ldots, \langle q_r, -eq_r\rangle$ by $\eta_1, \ldots, \eta_r$, respectively. It is easy to verify that the values of the total signature σ on these forms are independent (over $\mathbb{Z}$) elements of the group $\mathbb{Z}^r$. Hence the forms $\eta_1, \ldots, \eta_r$ are independent elements of the free abelian group A.

Suppose $\varphi \in WO_K$ and let $z_i = \sigma_i(\varphi)$, where $\sigma_i : WK \to \mathbb{Z}$ denotes the signature homomorphism at ∞_i. Note that $z_1 \equiv z_i \pmod 2$, for $i = 1, \ldots, r$. Consider

$$\psi = \varphi - \sum_{i=2}^{\rho} \frac{z_1 - z_i}{2}\eta_i - (z_1 - \sum_{i=2}^{\rho}\frac{z_1 - z_i}{2})\langle 1\rangle.$$

For every $i \in \{2, \ldots, \rho\}$ the discriminant $disc(\psi)$ is positive at ∞_i, because $\sigma_i(\psi) = 0$. Denote $y_i = \sigma_i(\psi)$, $i = 1, \ldots, r$.

We claim that $y_1 \equiv y_i \pmod 4$, for $i = \rho+1, \ldots, r$. Contrary to this suppose that $y_1 - y_i = 4k+2$ for some i. Suppose ψ has the diagonalization $\psi = \langle w_1, \ldots, w_m\rangle$. Then the difference between the number of 1's in the sequence $sign_{\infty_1}(w_1), \ldots, sign_{\infty_1}(w_m)$ and the number of 1's in the sequence $sign_{\infty_i}(w_1), \ldots, sign_{\infty_i}(w_m)$ is equal to $2k+1$. Hence

$$sign_{\infty_1}(disc(\psi)) \cdot sign_{\infty_i}(disc(\psi)) = -1.$$

This gives a contradiction, since $disc(\psi) \in K_{ev}$ and $|K_{ev}/K_{ev} \cap K_+| = 2^\rho$.

The total signature of the form

$$\psi_1 = \psi - \sum_{i=\rho+1}^{r} \frac{y_1 - y_i}{4}\eta_i - (y_1 - \sum_{i=\rho+1}^{r} \frac{y_1 - y_i}{2})\langle 1\rangle.$$

is equal to 0, hence $\psi_1 \in \mathfrak{N}(WO_K)$. Therefore φ is the sum of a certain element belonging to $\mathfrak{N}(WO_K)$ and a certain element of the form $\sum_i x_i\eta_i$, where $x_i \in \mathbb{Z}$.

COROLLARY 5.2. *If the rank of the group $K_{ev}/K_{ev} \cap K_+$ is equal to $\rho < r$ and e, b_i, q_i are as above, then*

$$WO_K = (\langle 1\rangle) \oplus \bigoplus_{i=2}^{\rho}(\langle 1, -b_i\rangle) \oplus \bigoplus_{i=\rho+1}^{r} (\langle q_i, -eq_i\rangle) \oplus \mathfrak{N}(WO_K).$$

From the above and from Corollary 3.1 we obtain the following decomposition of the group WO_K into direct sum of cyclic groups:

$$\begin{aligned} WO_K =&(\langle 1\rangle) \oplus \bigoplus_{i=2}^{\rho}(\langle 1, -b_i\rangle) \oplus \bigoplus_{i=\rho+1}^{r} (\langle q_i, -eq_i\rangle)\oplus \\ &\oplus \bigoplus_{i=1}^{c+t}(\langle 1, -a_i\rangle) \oplus \bigoplus_{i=u+1}^{g-1} (\langle\langle f, d_i\rangle\rangle), \end{aligned} \tag{11}$$

where a_i, f, d_i, e, b_i, q_i are as above and as in Section 3, and if $\rho = r$ or $u = g-1$, then in the decomposition the third or the last summand, respectively, does not occur.

Now we will describe the products of the generators of WO_K occurring in the decomposition (11). Similarly as in Section 3, to simplify the notation we will write $\varphi_i = \langle 1, -a_i\rangle$, $i = 1, \dots, c+t$, $\phi_i = \langle\langle f, d_i\rangle\rangle$, $i = u+1, \dots, g-1$ and moreover $\psi_i = \langle 1, -b_i\rangle$, $i = 1, \dots, \rho$, $\omega_i = \langle q_i, -eq_i\rangle$, $i = \rho+1, \dots, r$.

We start with determination of the product $\psi_i\psi_j = \langle\langle -b_i, -b_j\rangle\rangle$, for $i \neq j$. It is easy to verify, that

$$\sigma(\langle\langle -b_i, -b_j\rangle\rangle) = \sum_{k=\rho+1}^{r} x_k\sigma(2\langle 1\rangle - \omega_k),$$

where $x_k = \frac{1}{4}(1-sign_{\infty_k}(b_i))(1-sign_{\infty_k}(b_j))$. Thus the form $\eta = \langle\langle -b_i, -b_j\rangle\rangle - \sum_k x_k(2\langle 1\rangle - \omega_k)$ belongs to $\mathfrak{N}(WO_K)$ and so

$$disc(\eta) = (-e)^{\sum x_k} \in K_{ev} \cap K_+.$$

Let $disc(\eta) = \prod_{n=1}^{c+t} a_n^{l_n}$, where $l_n \in \{0,1\}$. Then the form

$$\eta_1 = \eta - \sum_{n=1}^{c+t} l_n\langle 1,\, -a_n\rangle$$

is an element of $\mathfrak{N}(W\mathcal{O}_K) \cap I^2K$ and it is completely determined by the value $H(\eta_1) \in \Gamma_K$. Therefore, if $H(\eta_1) = \prod_{m=1}^{u} \alpha_m^{y_m} \cdot \prod_{m=u+1}^{g-1} \alpha_m^{z_m}$, where $y_m, z_m \in \{0,1\}$, then

$$\psi_i\psi_j = \sum_{k=\rho+1}^{r} 2x_k\langle 1\rangle - \sum_{k=\rho+1}^{r} x_k\omega_k + \sum_{n=1}^{c+t} l_n\varphi_n + \\ + \sum_{m=1}^{u} 2y_m\varphi_m + \sum_{m=u+1}^{g-1} z_m\phi_m.$$

Clearly the product $\psi_i\psi_i$ is equal to $2\psi_i$.

Now we describe the product $\psi_i\omega_j = \langle 1,\, -b_i\rangle \cdot \langle q_j,\, -eq_j\rangle$. Observe that

$$\sigma(\psi_i\omega_j) = \sigma(2\psi_i) + \sum_{k=\rho+1}^{r} x_k\sigma(2\langle 1\rangle - \omega_k),$$

where $x_k = \frac{1}{2}(1 - sign_{\infty_k}(b_i)$. The form $\eta = \psi_i\omega_j - 2\psi_i - \sum x_k(2\langle 1\rangle - \omega_k)$ belongs to $\mathfrak{N}(W\mathcal{O}_K)$. If $disc(\eta) = \prod_{n=1}^{c+t} a_n^{l_n}$, then the form $\eta_1 = \eta - \sum_n l_n\langle 1,\, -a_n\rangle$ belongs to $\mathfrak{N}(W\mathcal{O}_K) \cap I^2K$ and is determined by $H(\eta_1)$. Similarly as in the previous case, we have

$$\psi_i\omega_j = 2\psi_i + \sum_{k=\rho+1}^{r} 2x_k\langle 1\rangle - \sum_{k=\rho+1}^{r} x_k\omega_k + \sum_{n=1}^{c+t} l_n\varphi_n + \\ + \sum_{m=1}^{u} 2y_m\varphi_m + \sum_{m=u+1}^{g-1} z_m\phi_m,$$

where $H(\eta_1) = \prod_{m=1}^{u} \alpha_m^{y_m} \cdot \prod_{m=u+1}^{g-1} \alpha_m^{z_m}$.

Let $i, j \in \{\rho+1, \ldots, r\}$. If $i \neq j$, then the total signature of the form $\eta_1 = \omega_i\omega_j - 2\omega_i - 2\omega_j + 4\langle 1\rangle$ is equal to 0. Hence $\eta_1 \in \mathfrak{N}(W\mathcal{O}_K) \cap I^2K$ and we have

$$\omega_i\omega_j = -4\langle 1\rangle + 2\omega_i + 2\omega_j + \sum_{m=1}^{u} 2y_m\varphi_m + \sum_{m=u+1}^{g-1} z_m\phi_m,$$

where the coefficients $y_m, z_m \in \{0,1\}$ are described by the equality $H(\eta_1) = \prod_{m=1}^{u} \alpha_m^{y_m} \cdot \prod_{m=u+1}^{g-1} \alpha_m^{z_m}$.

If $i = j$, then analogously

$$\omega_i \omega_i = 4\langle 1\rangle + \sum_{m=1}^{u} 2y_m \varphi_m + \sum_{m=u+1}^{g-1} z_m \phi_m,$$

where the coefficients $y_m, z_m \in \{0,1\}$ are determined by the value of $H(\omega_i\omega_i - 1\langle 1\rangle)$.

The products $\psi_i\varphi_j, \omega_i\varphi_j$ belong to $\mathfrak{N}(W\mathcal{O}_K) \cap I^2K$ and are determined by the values of $H(\psi_i\varphi_j)$ and $H(\omega_i\varphi_j)$, respectively, similarly as above. The products $\psi_i\phi_j, \omega_i\phi_j$ belong to $\mathfrak{N}(W\mathcal{O}_K) \cap I^3K = 0$, so they are all equal to 0.

6. Quadratic number fields

In this section we determine the structure of the Witt ring $W\mathcal{O}_K$ in the case when K is a quadratic number field. A similar description has been found in [M].

Assume that $K = \mathbb{Q}(\sqrt{m})$, where m is a square-free integer, and let $p_1, \dots, p_\tau$ be all pairwise distinct prime divisors of the discriminant of K. We agree that $p_1 = 2$ whenever $m \equiv 3 \pmod 4$. The Gauss Genus Theorem states that $t = \tau - 1$. It is easy to see that the sets

$$\begin{aligned} \{-1, p_1, \dots, p_t\}, &\quad \text{when } m < 0 \text{ and } m \neq -1,\\ \{p_1, \dots, p_t\}, &\quad \text{when } m > 0 \end{aligned}$$

form a basis of the group $K_{\mathrm{ev}} \cap K_+/\dot{K}^2$. When $K = \mathbb{Q}(\sqrt{-1})$, the set $\{2\}$ forms a basis of the group $K_{\mathrm{ev}} \cap K_+/\dot{K}^2$.

First we consider the case when K is imaginary quadratic field (i.e. $m<0$). The level of the field K is determined as follows:

$$s = \begin{cases} 1 & \text{when} \quad m = -1, \\ 2 & \text{when} \quad m \not\equiv 1 (\text{mod } 8) \text{ and } m \neq -1, \\ 4 & \text{when} \quad m \equiv 1 (\text{mod } 8). \end{cases}$$

If $m = -1$, (i.e. $K = \mathbb{Q}(\sqrt{-1})$), then $g = 1$ and (9) gives

$$W\mathcal{O}_K = (\langle 1\rangle) \oplus (\langle 1, -2\rangle) \cong (\mathbb{Z}/2\mathbb{Z}) \oplus (\mathbb{Z}/2\mathbb{Z}). \tag{12}$$

The group $W\mathcal{O}_K$ is an elementary abelian 2-group and the product $\langle 1, -2\rangle \cdot \langle 1, -2\rangle$ is equal to $2\langle 1, -2\rangle = 0$.

Let $m \neq -1$ and $m \not\equiv 1 \pmod 8$. In this case the field K has one dyadic prime and from (8) we obtain the decomposition

$$(13) \qquad WO_K = (\langle 1\rangle) \oplus \bigoplus_{i=1}^{t} (\langle 1,\, -p_i\rangle) \cong (\mathbb{Z}/4\mathbb{Z}) \oplus (\mathbb{Z}/2\mathbb{Z})^t.$$

The products $\langle 1,\, p_i\rangle \cdot \langle 1,\, p_j\rangle$ vanish, because $\mathfrak{N}\,(WO_K) \cap I^2K = 0$.

Now assume that $m \equiv 1 \pmod 8$. Then there are 2 dyadic primes $\mathfrak{p}_1, \mathfrak{p}_2$ in the field K and $-1 \notin D_K\langle 1,\, 1\rangle$. Hence $u = 1$. Take

$$p_i' = \begin{cases} p_i & \text{when } p_i \equiv 1 \pmod 4, \\ -p_i & \text{when } p_i \equiv 3 \pmod 4. \end{cases}$$

The set $\{-1, p_1', \dots, p_t'\}$ forms a basis of the group $K_{\mathrm{ev}} \cap K_+/\dot{K}^2$ and $p_1', \dots, p_t' \in D_K\langle 1,\, 1\rangle$. From (7) we have

$$(14) \qquad WO_K = (\langle 1\rangle) \oplus \bigoplus_{i=1}^{t} (\langle 1,\, -p_i'\rangle) \cong (\mathbb{Z}/8\mathbb{Z}) \oplus (\mathbb{Z}/2\mathbb{Z})^t.$$

Because $H(\langle\langle -p_i',\, -p_j'\rangle\rangle) = (p_i', p_j')_{\mathfrak{p}_1} = 1$, we have

$$\langle 1,\, -p_i'\rangle \cdot \langle 1,\, -p_j'\rangle = 0$$

for all $i, j \in \{1, \dots, t\}$.

Now we consider the case when K is a real quadratic field (i.e. $m > 0$). Then $r = 2$, i.e. the field K has 2 real infinite primes ∞_1, ∞_2. The 2-rank of the group $K_{\mathrm{ev}}/K_{\mathrm{ev}} \cap K_+$ is equal

$$\rho = \begin{cases} 1 & \text{when} \quad -1 \notin N(K), \\ 2 & \text{when} \quad -1 \in N(K), \end{cases}$$

where $N(K)$ denotes the norm group of the extension $K/\mathbb{Q}$ (see [Cz1]). The condition $-1 \in N(K)$ can be replaced by the conditions $p_i \equiv 1, 2 \pmod 4$ for $i = 1, \dots, t+1$.

Assume that $-1 \in N(K)$. Then there exists an element $b \in K_{\mathrm{ev}}$ such that b is positive at ∞_1 and negative at ∞_2 (cf. [Cz1]).

If $m \not\equiv 1 \pmod 8$, then $g = 1$ and (11) gives

$$(15) \qquad WO_K = (\langle 1\rangle) \oplus (\langle 1,\, -b\rangle) \oplus \bigoplus_{i=1}^{t} (\langle 1,\, -p_t\rangle) \cong \mathbb{Z}^2 \oplus (\mathbb{Z}/2\mathbb{Z})^t.$$

The products $\langle 1, -p_i\rangle \cdot \langle 1, -p_j\rangle$, $\langle 1, -b\rangle \cdot \langle 1, -p_j\rangle$ are equal to 0, because in this case $\mathfrak{N}(W\mathcal{O}_K) \cap I^2K$ is trivial. Clearly $\langle 1, -b\rangle \cdot \langle 1, -b\rangle = 2\langle 1, -b\rangle$.

If $m \equiv 1 \pmod 8$, then $p_i \equiv 1 \pmod 4$ for every $i \in \{1, \dots, t+1\}$, so $u = 0$. In this case there are 2 dyadic primes $\mathfrak{p}_1, \mathfrak{p}_1$ in K. Hence from (11) we obtain

$$W\mathcal{O}_K = (\langle 1\rangle) \oplus (\langle 1, -b\rangle) \oplus \bigoplus_{i=1}^{t}(\langle 1, -p_t\rangle) \oplus (\langle\langle f, d\rangle\rangle) \cong \mathbb{Z}^2 \oplus (\mathbb{Z}/2\mathbb{Z})^{t+1}. \tag{16}$$

Here f, d are any elements of K such that $-f$ is totally positive and $(-f, -d)_{\mathfrak{p}_1} = -1$. Observe that $H(\langle\langle -p_i, -p_j\rangle\rangle) = (p_i, p_j)_{\mathfrak{p}_1} = 1$ and $H(\langle\langle -b, -p_j\rangle\rangle) = (b, p_j)_{\mathfrak{p}_1} = 1$. Thus we have $\langle 1, -p_i\rangle \cdot \langle 1, -p_j\rangle = 0$ and $\langle 1, -b\rangle \cdot \langle 1, -p_j\rangle = 0$. The products of the elements $\langle 1, -b\rangle$, $\langle 1, -p_i\rangle$ by the form $\langle\langle f, d\rangle\rangle$ are equal to 0, because they belong to $\mathfrak{N}(W\mathcal{O}_K) \cap I^3K = 0$. Similarly as above we have $\langle 1, -b\rangle \cdot \langle 1, -b\rangle = 2\langle 1, -b\rangle$.

Now assume that $-1 \notin N(K)$. Take

$$e = \begin{cases} -1 & \text{when } m \not\equiv 7 \pmod 8, \\ -2 & \text{when } m \equiv 7 \pmod 8). \end{cases}$$

It is easy to see that $-e \in K_{\mathrm{ev}} \cap K_+$ and e is a local nonsquare at every dyadic prime of K. From Corollary 5.2 it follows that there exists an element $q \in K$ such that

$$W\mathcal{O}_K = (\langle 1\rangle) \oplus (\langle q, -eq\rangle) \oplus \mathfrak{N}(W\mathcal{O}_K). \tag{17}$$

If $m \not\equiv 1 \pmod 8$, then $g = 1$ and from (11) it follows that

$$W\mathcal{O}_K = (\langle 1\rangle) \oplus (\langle q, -eq\rangle) \oplus \bigoplus_{i=1}^{t}(\langle 1, -p_i\rangle) \cong \mathbb{Z}^2 \oplus (\mathbb{Z}/2\mathbb{Z})^t. \tag{18}$$

In this case we have $\mathfrak{N}(W\mathcal{O}_K) \cap I^2K = 0$, hence the products $\langle q, -eq\rangle \cdot \langle 1, -p_i\rangle$ and $\langle 1, -p_i\rangle \cdot \langle 1, -p_j\rangle$ are equal to 0. It is easy to verify that $\langle q, -eq\rangle \cdot \langle q, -eq\rangle = 4\langle 1\rangle$.

It remains to consider the case when $-1 \notin N(K)$ and $m \equiv 1 \pmod 8$. In this case there exists a prime number dividing m, which is congruent to 3 modulo 4. We can assume that $p_1 \equiv 3 \pmod 4$. The field K contains 2 dyadic prime ideals $\mathfrak{p}_1, \mathfrak{p}_2$. Clearly $(-1, p_1)_{\mathfrak{p}_1} = -1$, hence p_1 does not belong to $D_K\langle 1, 1\rangle$. Thus $u = 1$ and $\langle 1, -p_1\rangle$ is the element of order 4 of the the group $W\mathcal{O}_K$. Take $p_1' = p_1$ and for $i \in \{2, \dots, t\}$,

$$p_i' = \begin{cases} p_i & \text{when } p_i \equiv 1 \pmod 4, \\ p_1 p_i & \text{when } p_i \equiv 3 \pmod 4). \end{cases}$$

Then the set $\{p'_1, \dots, p'_t\}$ is a basis of the group $K_{\mathrm{ev}} \cap K_+/\dot{K}^2$ and $p'_2, \dots, p'_t \in D_K\langle 1, 1\rangle$. From (11) we have

$$\begin{aligned} W\mathcal{O}_K &= (\langle 1\rangle) \oplus (\langle q, q\rangle) \oplus \bigoplus_{i=1}^{t} (\langle 1, -p_i\rangle) \\ &\cong \mathbb{Z}^2 \oplus \mathbb{Z}/4\mathbb{Z} \oplus (\mathbb{Z}/2\mathbb{Z})^{t-1}. \end{aligned}$$

Observe that for all $i, j \in \{2, \dots, t\}$ we have

$$H(\langle\langle -p'_1, -p'_i\rangle\rangle) = (p'_1, p'_i)_{\mathfrak{p}_1} = 1, \quad H(\langle\langle -p'_i, -p'_j\rangle\rangle) = (p'_i, p'_j)_{\mathfrak{p}_1} = 1,$$

$$H(\langle q, q\rangle \cdot \langle 1, -p'_i\rangle) = (-1, p'_i)_{\mathfrak{p}_1} = 1.$$

Hence the products $\langle 1, -p'_1\rangle \cdot \langle 1, -p'_i\rangle$, $\langle 1, -p'_i\rangle \cdot \langle 1, -p'_j\rangle$, $\langle q, q\rangle \cdot \langle 1, -p'_i\rangle$ are all equal to 0. Clearly $\langle q, q\rangle \cdot \langle q, q\rangle = 4\langle 1\rangle$ and $\langle 1, -p'_1\rangle \cdot \langle 1, -p'_1\rangle = 2\langle 1, -p'_1\rangle$.

The results of this section allow us to find arithmetical conditions for the existence of an isomorphism of Witt rings $W\mathcal{O}_K \to W\mathcal{O}_L$ for quadratic number fields K and L. An isomorphism $\Psi : W\mathcal{O}_K \to W\mathcal{O}_L$ is called a *strong isomorphism* of Witt rings, if it preserves the dimensions of anisotropic forms.

COROLLARY 6.1. *Let K, L be imaginary quadratic number fields. There exists a strong isomorphism Witt rings $W\mathcal{O}_K \to W\mathcal{O}_L$ if and only if the following two conditions are satisfied:*

(1) $s(K) = s(L)$,

(2) $t(K) = t(L)$,

COROLLARY 6.2. *Let K, L be real quadratic number fields. There exists a strong isomorphism Witt rings $W\mathcal{O}_K \to W\mathcal{O}_L$ if and only if the following three conditions are satisfied:*

(1) $g(K) = g(L)$,

(2) $t(K) = t(L)$,

(3) $-1 \in N(K) \iff -1 \in N(L)$.

7. Cubic and biquadratic number fields

As we have seen in the preceding sections, to determine the structure of the Witt ring $W\mathcal{O}_K$ we need a suitable basis of the group $K_{\mathrm{ev}}/\dot{K}^2$. Unfortunately, no method of finding a basis of the group $K_{\mathrm{ev}}/\dot{K}^2$ in the general case is known. On the other hand in some simple cases it is possible to find a basis. In this section we will determine the structure of the Witt rings $W\mathcal{O}_K$ in some pure cubic number fields and some biquadratic number fields.

In the examples of cubic fields we only complete the results of the paper [Sh].

EXAMPLE 7.1. Let $K = \mathbb{Q}(\sqrt[3]{3})$. Write $w = \sqrt[3]{3}$. The number $\epsilon = w^2 - 2$ is the positive fundamental unit of K, so $\epsilon \in K_{\text{ev}} \cap K_+$. From [Sh] it follows that $\epsilon \notin D_K\langle 1, 1\rangle$. Hence the ideal class group in the narrow sense is trivial (i.e. $t = 0$). The field K has one real prime ($r = 1$), one pair of complex primes ($c = 1$) and two dyadic primes. Therefore from (11) we obtain

$$W\mathcal{O}_K = (\langle 1\rangle) \oplus (\langle 1, -\epsilon\rangle) \cong \mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$$

Clearly the product $\langle 1, -\epsilon\rangle \cdot \langle 1, -\epsilon\rangle$ is equal to $2\langle 1, -\epsilon\rangle$.

Similar results can be obtained for the cubic fields $\mathbb{Q}(\sqrt[3]{5})$ and $\mathbb{Q}(\sqrt[3]{7})$ (for details see [Sh]).

Now we determine the structure $W\mathcal{O}_K$ for some biquadratic number fields.

EXAMPLE 7.2. Let p be a prime number congruent to 3 mod 8. Let $K = \mathbb{Q}(\sqrt{-2}, \sqrt{2p})$. The field K is totally imaginary, so $c = 2$. The Theorem 20.3 in [CH] states that the class number of K is odd, hence $t = 0$. Observe that the local degree $[\mathbb{Q}_2(\sqrt{-2}, \sqrt{2p}) : \mathbb{Q}_2]$ is equal to 4 and the prime number 2 ramifies in K. Thus there is just one dyadic prime in K and $2 \in K_{\text{ev}}$. Therefore the set $\{-1, 2\}$ forms a basis of $K_{\text{ev}}/\dot{K}^2$. It is easy to verify that the level of K is equal to 2. From (8) we have

$$W\mathcal{O}_K = (\langle 1\rangle) \oplus (\langle 1, -2\rangle) \cong \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}.$$

The product $\langle 1, -2\rangle \cdot \langle 1, -2\rangle$ is equal to 0.

From the above example and (13) we obtain

COROLLARY 7.1. *Let p_1 be a prime congruent to 1 mod 4 and p_2 be a prime congruent to 3 mod 8. Then for the fields $K = \mathbb{Q}(\sqrt{-p_1})$ and $L = \mathbb{Q}(\sqrt{-2}, \sqrt{2p_2})$ the Witt rings $W\mathcal{O}_K$ and $W\mathcal{O}_L$ are strongly isomorphic.*

EXAMPLE 7.3. Let p be a prime congruent to 3 mod 8 and let $K = \mathbb{Q}(\sqrt{-1}, \sqrt{p})$. From [CH, Theorem 20.3] it follows that the class number of K is odd (i.e. t=0). It is easy to verify that the field K has a unique dyadic prime, $s(K) = 1$ and $2, p \in K_{\text{ev}}$. Therefore (9) gives the decomposition

$$W\mathcal{O}_K = (\langle 1\rangle) \oplus (\langle 1, -2\rangle) \oplus (\langle 1, -p\rangle) \cong (\mathbb{Z}/2\mathbb{Z})^3.$$

Moreover, all the products of 2-dimensional generators vanish, because $\mathfrak{N}(W\mathcal{O}_K) \cap I^2K$ is trivial.

References

[Cz1] A. Czogała, *On reciprocity equivalence of quadratic number fields*, Acta Arith., **58** (1991), 365–387.

[Cz2] A. Czogała, *Witt equivalence of rings of algebraic integers*, (in prep.).

[CH] P. E. Conner, J. Hurrelbrink, *Class number parity*, Ser. Pure Math. 8, World Sci., Singapore (1988).

[L] S. Lang, *Algebraic Number Theory*, Massachusetts, Addison-Wesley (1970).

[MH] J. Milnor, D. Husemoller, *Symmetric Bilinear Forms*, Springer Verlag, Berlin (1973).

[M] R. Münstermann, *Der Wittring des Rings der ganzen Zahlen eines quadratischen Zahlkörpers*, Diplomarbeit, Bielefeld (1983).

[OM] O. T. O'Meara, *Introduction to Quadratic Forms*, Springer Verlag, Berlin (1973).

[Sh] P. Shastri, *Witt groups of algebraic integers*, J. Number Theory, **30** (1988), 243–266.

Instytut Matematyki
Uniwersytet Śląski
Bankowa 14
40–007 Katowice
Poland

e-mail:
czogala@ux2.math.us.edu.pl